Data Protection and Brexit

Law enforcement processing: Five steps to take

1 Continue to comply

Continue to comply with Part 3 of the DPA 2018, and follow current ICO guidance on law enforcement processing.

2 Transfers to the UK

Review your data flows and identify where you receive data from the EU. Talk to your European partners about whether they need you to put any additional safeguards in place to ensure data can continue to flow.

3 Transfers from the UK

Review your data flows and identify where you transfer data to the EU, so that you can document the new basis for those transfers.

4 Documentation

Review your privacy information, internal records and logs to identify any details that will need updating when the UK leaves the EU.

5 Organisational awareness

Make sure key people in your organisation are aware of these issues. Include these steps in any planning for leaving the EU, and keep up to date with the latest guidance.

Introduction

This checklist highlights five steps law enforcement authorities can take to prepare for data protection compliance if the UK leaves the EU without a deal.

This guidance is for 'competent authorities' processing personal data for law enforcement purposes under Part 3 of the Data Protection Act 2018 (DPA 2018). If you are not sure if this applies to you, read our guidance on which data protection regime applies.

If you are not a competent authority, or you are a competent authority processing for non-law enforcement purposes (eg your HR records), read our separate guidance on GDPR and Brexit.

If you are a UK competent authority, you won't need to do much to prepare in terms of your day-to-day domestic processing. The relevant law enforcement processing regime in Part 3 of the DPA 2018 will continue to apply after we leave the EU. Therefore, your best preparation is to ensure you are complying with the DPA 2018 now.

You may however need to ensure 'appropriate safeguards' are in place to maintain any data flows to you from the EU. You may also need to review your documentation for transferring data to the EU.

You can use this checklist to help work out whether you will be affected once we leave the EU, and take some key steps to prepare.

1 Continue to comply

You should continue to comply with Part 3 of the DPA 2018, and follow current ICO guidance on law enforcement processing.

The DPA 2018 is part of UK law and will remain in place. There will be some minor technical amendments to the transfers provisions of Part 3 to reflect the fact that the UK is no longer a member state after exit day, but these changes will not affect your day-to-day domestic processing.

This means the first and most important step is to ensure you continue to comply with the principles, rights and obligations set out in Part 3 of the DPA 2018. Our current guidance remains relevant and can help you to comply. We will continue to review and update it regularly to reflect any changes or developments in practice.

2 Transfers to the UK

Review your data flows and identify where you receive data from the EU. Talk to your European partners about whether they want you to put any additional safeguards in place to ensure data can continue to flow.

Once we leave the EU, we will become a 'third country' for EU data protection purposes. If you receive personal data from a law enforcement partner in the EU, this means the sender will need to comply with the transfer provisions under their national data protection law (which are likely to be similar to the provisions in Part 3 of the DPA 2018).

If the EU makes a formal 'adequacy decision' that the UK regime offers an adequate level of protection, there will be no need for specific safeguards. However, if we leave the EU on 29 March 2019 without a deal, there will not yet be such a decision in place. So in practice this means the EU sender needs to make sure there are other appropriate safeguards in place – likely either through a contract or other binding legal instrument, or by making their own assessment of appropriate safeguards. The sender can take into account the protection provided by the DPA 2018 itself when making this assessment.

If you receive personal data from other types of organisations in the EU or EEA who are subject to the GDPR, the sender will need to comply with the transfer provisions of the GDPR. You may want to consider putting standard contractual clauses (SCCs) in place to ensure adequate safeguards in these cases. We have produced an interactive tool to help you use the SCCs.

3 Transfers from the UK

Review your data flows and identify where you transfer data to the EU, so that you can document the new basis for those transfers.

Transfers from the UK to the EU

The UK government has confirmed that there will be a transitional adequacy decision in place to cover transfers to EU member states and Gibraltar. (This will not extend to EEA countries outside the EU, where you should continue to consider other safeguards).

This means that you will be able to continue to send personal data from the UK to your law enforcement partners in the EU, as long as you can show the transfer is necessary for law enforcement purposes. You can also transfer personal data to non-law enforcement bodies in the EU if you can meet some additional conditions, but you will need to notify the ICO.

For more information, see our guidance on international transfers for competent authorities, bearing in mind that EU countries will be third countries (with an adequacy decision) after we leave the EU.

Transfers from the UK to countries outside the EU

Rules on transfers to other countries outside the EU will remain the same in practice. At this stage you don't need to take any specific additional steps.

For more information on the rules on transfers outside the EU, see our guidance on international transfers for competent authorities. This will be updated to reflect the technical changes to the UK rules (in particular on new UK adequacy regulations) when we leave the EU.

4 Documentation

Review your privacy information, internal processing records and logs to identify any details that will need updating when the UK leaves the EU.

The requirements for privacy notices, documentation and logging are unlikely to change. But you need to review what you say about international transfers and make sure it includes details of transfers to the EU. You may also need to identify any references to EU law, EU membership or other EU terminology, and be ready to make changes to reflect the UK's status outside the EU by exit date.

You may also need to review existing data protection impact assessments, if they involve data transfers between the UK and EU.

5 Organisational awareness

Make sure key people in your organisation are aware of these issues. Include these steps in any planning for leaving the EU, and keep up to date with the latest guidance.

Key people in your organisation need to be aware of the ongoing importance of data protection compliance, as well as specific implications for data flows. If you have significant data transfers to and from the EU, you can plan ahead. You may find it more difficult to ensure continuity if you leave your preparations until the last minute.

We will keep this guidance under review and update it if anything changes, or more details become available. We will also update our Guide to Law Enforcement Processing when we leave the EU to reflect the amendments to the DPA 2018.